Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) An apparatus arranged to accept digital data as an input and to process the data according to one of either the Secure Hash Algorithm (SHA-1) or Message Digest (MD5) algorithm to produce a fixed length output word, the apparatus comprising:

a plurality of rotational registers ~~for storing~~ coupled to a read bus to receive and store data, one of said rotational registers arranged to receive the input data; ~~and~~

data stores coupled to the read bus for initialization of some of said plurality of rotational registers according to whether the SHA-1 or MD5 algorithm is used, said data stores including fixed data relating to SHA-1 and MD5 operation; ~~and~~

a plurality of dedicated combinatorial logic circuits having inputs coupled to the read bus and outputs coupled to the write bus and arranged to perform logic operations on data stored in selected ones of said plurality of registers and to output to the write bus; and

a plurality of temporary data storage registers having inputs coupled to the write bus and outputs coupled to the read bus, an output of one of the temporary data storage registers comprising an output of the apparatus for the fixed length output word.

2. (Previously Presented) The apparatus of claim 1 wherein the register arranged to receive the input data is arranged to receive said input data serially.

3. (Currently Amended) The apparatus of claim 1 wherein the registers and combinatorial logic circuits are interconnected for communication via ~~a pair of~~ the read and write data busses.

4. (Previously Presented) The apparatus of claim 3 wherein the registers and combinatorial logic circuits are connected to write to a respective bus via respective tristate buffers.

5. (Previously Presented) The apparatus of claim 1 wherein the apparatus includes a control circuit arranged to generate individually gated clock signals for each register.

6. (Previously Presented) The apparatus of claim 5 wherein said control circuit is further arranged to generate individual enabling signals to control the tristate buffers.

7. (Previously Presented) The apparatus of claim 1 wherein the rotational registers are arranged to be multiplexed prior to connection to a tristate buffer.

8. (Previously Presented) The apparatus of claim 1 wherein the combinatorial logic circuits include a copy circuit, a shift left circuit, a NOT circuit, an ADD circuit, an OR circuit, an AND circuit and an XOR circuit.

9. (Previously Presented) The apparatus of claim 1 wherein the apparatus is implemented as an integrated circuit.

10. (Previously Presented) The apparatus of claim 1 wherein the apparatus further includes circuitry arranged to perform digital signature creation or authentication.

11. (Currently Amended) A circuit, comprising:

a plurality of data storage registers ~~for storing~~ coupled to a read bus to receive and store data to be processed;

a plurality of shift registers for temporary data storage and having inputs coupled to a write bus and outputs coupled to the read bus, an output of one of the shift registers comprising an output of the circuit;

a plurality of logic circuits having inputs coupled to the read bus and outputs coupled to the write bus and for performing operations on data and to output to the write bus; and

a control circuit configured to control the data storage registers, the shift registers, and the logic circuits to selectively perform MD5 and SHA-1 operations on data.

12. (Currently Amended) The circuit of claim 11, further comprising a plurality of initialization storage registers coupled to the read bus and adapted to store and output initialization data for the MD5 and SHA-1 operations.

13. (Currently Amended) The circuit of claim 12~~,~~ ~~comprising a~~ wherein the read bus and ~~a~~ the write bus are selectively coupleable to the plurality of data storage registers, the plurality of shift registers, and the plurality of logic circuits by the control circuit.

14. (Previously Presented) The circuit of claim 11, further comprising a multiplexer to multiplex outputs of the plurality of shift registers to the read bus.

15. (Currently Amended) A circuit, comprising:

means for storing data coupled to a read bus to receive and store data to be processed;

means for temporarily storing the data to be processed and having inputs coupled to a write bus and outputs coupled to the read bus, an output of one of the shift registers comprising an output of the circuit;

means for performing combinatorial logic operations having inputs coupled to the read bus and outputs coupled to the write bus and arranged to perform logic operations on the data and output results to the write bus; and

means for controlling coupling of the data storage means, the temporary data storage means, and the means for performing combinatorial logic operations to the read and write busses to selectively perform MD5 and SHA-1 operations on the data.

16. (Currently Amended) The circuit of claim 15, further comprising means for storing data coupled to the read bus, the data used to initialize the circuit to perform MD5 and SHA-1 operations in response to commands from the control means.

17. (Previously Presented) The circuit of claim 15, further comprising means for multiplexing outputs from the temporary data storage registers to the read bus in response to commands from the control means.

18. (Currently Amended) The circuit of claim 17 wherein the temporary data storage means is configured to receive a stream of data, and the circuit ~~further comprises an~~ generates on the output ~~on which is generated~~ data of a fixed length.

19. (Currently Amended) A dual hash algorithm circuit, comprising:

a first bank and a second bank of data storage registers having inputs coupled to a write bus and outputs coupled to a read bus;

a first bank and a second bank of circular shift registers coupled to a read bus to receive and store data, including at least one register to receive a data stream as input to the circuit;

a bank of initialization data registers coupled to the read bus;

a bank of temporary data registers coupled to the read bus;

a plurality of combinatorial logic circuits having inputs coupled to the read bus and outputs coupled to the write bus; and

~~a read bus and a write bus;~~

a control system for selectively coupling and uncoupling the first bank and second bank of data storage registers, the first bank and second bank of circular shift registers, the bank of initialization data registers, the bank of temporary data registers, and the plurality of combinatorial logic circuits to the respective read bus and the write bus to selectively perform MD5 and SHA-1 operations on the data and to output data of a fixed length in accordance with the selected MD5 and SHA-1 operations.

20. (Currently Amended) The circuit of claim 19 wherein the control system comprises a control circuit and tristate buffers to couple and uncouple the first bank and second bank of data storage registers, the first bank and second bank of circular shift registers, the bank of initialization data registers, the bank of temporary data registers, and the plurality of combinatorial logic circuits to the respective read and write busses in response to the control circuit.

21. (Previously Presented) The circuit of claim 19, further comprising a multiplexer configured to multiplex outputs from the first bank and second bank of circular shift registers to the read bus.